Construction of Error-Correcting Codes for Random Network Coding

Tuvi Etzion
Department of Computer Science
Technion, Haifa 32000, Israel
e-mail: etzion@cs.technion.ac.il
phone: 04-8294311, fax: 04-8293900

Natalia Silberstein
Department of Computer Science
Technion, Haifa 32000, Israel
e-mail: natalys@cs.technion.ac.il
phone: 04-8294952, fax: 04-8293900

Abstract — **In this work we present error-correcting codes for random network coding based on rank-metric codes, Ferrers diagrams, and puncturing. For most parameters, the constructed codes are larger than all previously known codes.**

Classification: Information Theory and Coding Theory

I. Introduction

The *projective space* of order n over finite field $\mathbb{F}_q = GF(q)$, denoted by $\mathcal{P}_q(n)$, is the set of all subspaces of the vector space $\mathbb{F}_q^n$. $\mathcal{P}_q(n)$ is a metric space with the distance function $d_S(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$, for all $U, V \in \mathcal{P}_q(n)$. A code in the projective space is a subset of $\mathcal{P}_q(n)$. Koetter and Kschischang [4] showed that codes in $\mathcal{P}_q(n)$ are useful for correcting errors and erasures in random network coding. If the dimension of each codeword is a given integer $k \leq n$ then the code forms a subset of a the Grassmannian $\mathcal{G}_q(n,k)$ and called a *constant-dimension code*.

The *rank distance* between $X,Y \in \mathbb{F}_q^{m\times t}$ is defined by $d_R(X,Y) = \text{rank}(X - Y)$. It is well known [2] that the rank distance is a metric. A code $C \subseteq F_q^{m\times t}$ with the rank distance is called a *rank-metric code*. The connection between the rank-metric codes and codes in $\mathcal{P}_q(n)$ was explored in [3, 4, 6].

We represent a k-dimensional subspace $U \in \mathcal{P}_q(n)$ by a $k \times n$ matrix, in *reduced row echelon form*, whose rows form a basis for U. The *echelon Ferrers form* of a binary vector v of length n and weight k, $EF(v)$, is a $k \times n$ matrix in reduced row echelon form with leading entries (of rows) in the columns indexed by the nonzero entries of v and " $\bullet$ " (will be called *dot*) in the "arbitrary" entries.

Example 1. *Let $v = 0110100$. Then*

$$EF(v) = \begin{pmatrix} 0 & 1 & 0 & \bullet & 0 & \bullet & \bullet \\ 0 & 0 & 1 & \bullet & 0 & \bullet & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet & \bullet \end{pmatrix}.$$

Let S be the sub-matrix of $EF(v)$ that consists of all its columns with dots. A matrix M over $\mathbb{F}_q$ is said to be in $EF(v)$ if M has the same size as S and if $S_{i,j} = 0$ implies that $M_{i,j} = 0$. $EF(v[M])$ will be the matrix that result by placing the matrix M instead of S in $EF(v)$.

II. Construction of Constant Dimension Codes

Let $\mathcal{C}$ be a constant-weight code of length n, constant weight k, and minimum Hamming distance $d_H = 2\delta$. Let C_v be the largest rank-metric code with the minimum distance $d_R = \delta$, such that all its codewords are in $EF(v)$. Now define code $\mathbb{C} = \bigcup_{v\in\mathcal{C}} \{EF(v[c]) : c \in C_v\}$.

Lemma 1. *For all $v_1, v_2 \in \mathcal{C}$ and $c_i \in EF(v_i), i = 1,2$, $d_S(EF(v_1[c_1]), EF(v_2[c_2])) \geq d_H(v_1,v_2)$. If $d_H(v_1,v_2) = 0$, then $d_S(EF(v_1[c_1]), EF(v_2[c_2])) = 2d_R(c_1,c_2)$.*

Corollary 1. *$\mathbb{C} \in \mathcal{G}_q(n,k)$ and $d_S(\mathbb{C}) = 2\delta$.*

Theorem 1. *Let $C_v \subseteq \mathbb{F}_q^{m\times t}$ be a rank-metric code with $d_R(C_v) = \delta$, such that all its codewords are in $EF(v)$ for some binary vector v. Let S be the sub-matrix of $EF(v)$ which corresponds to the dots part of $EF(v)$. Then the dimension of C_v is upper bounded by the minimum between the number of dots in the last $m - \delta + 1$ rows of S and the number of dots in the first $t - \delta + 1$ columns of S.*

Constructions for codes which attain the bound of Theorem 1 for most important cases are given in [1]. Examples are given in the following table (see [5] for details):

q	n	k	d_s	$\lvert\mathbb{C}\rvert$
2	6	3	4	71
2	7	3	4	289
2	8	4	4	4573

III. Error-Correcting Projective Space Codes

Let $\mathbb{C} \in \mathcal{G}_q(n,k)$ with $d_S(\mathbb{C}) = 2\delta$. Let Q be an $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$ and $v \in \mathbb{F}_q^n$ such that $v \notin Q$. Let $\mathbb{C}' = \mathbb{C}_1 \cup \mathbb{C}_v$, where $\mathbb{C}_1 = \{c \in \mathbb{C} : c \subseteq Q\}$ and $\mathbb{C}_v = \{c \cap Q : c \in \mathbb{C},\ v \in c\}$.

Lemma 2. *$\mathbb{C}' \in \mathcal{P}_q(n-1)$ and $d_S(\mathbb{C}') = 2\delta - 1$.*

By applying this *puncturing* method with the 7-dimensional subspace Q whose generator matrix is

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

and the vector $v = 10000001$, on the code with size 4573, and minimum distance 4, in $\mathcal{G}_2(8,4)$, we were able to obtain a code with minimum distance 3 and size 573 in $\mathcal{P}_2(7)$.

References

[1] T. Etzion and N. Silberstein, Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams, in preparation.

[2] E. M. Gabidulin, Theory of codes with maximum rank distance, *Problems on Inform. Trans.*, 21(1):1–12, Jan.1985.

[3] M. Gadouleau and Z. Yan, On the connection between optimal constant-rank codes and optimal constant-dimension codes, 2008, available at http://arxiv.org/abs/0803.2262.

[4] R.Koetter and F.R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory*, to appear.

[5] N. Silberstein, Coding theory in projective space, proposal, 2008, available at http://arxiv.org/abs/0805.3528.

[6] D. Silva, F. R. Kschischang, and R. Koetter, A rank-metric approach to error control in random network coding, *ITW, Bergen, Norway*, pages 73–79, July 1-6, 2007.